International Journal of Communication 11(2017), 731–739 1932–8036/20170005

Digital Citizenship and Surveillance Society

Introduction

ARNE HINTZ
LINA DENCIK
KARIN WAHL-JORGENSEN
Cardiff University, UK

Digital citizenship is typically defined as the (self-)enactment of people's role in society through the use of digital technologies. It therefore has empowering and democratizing characteristics. However, as shown by this Special Section, the context of datafication and ubiquitous data collection and processing complicates this picture. The Snowden revelations have demonstrated the extent to which both state agencies and Internet companies monitor the activities of digital citizens and how the balance of power shifts accordingly. This editorial introduction outlines the challenges and transformations of digital citizenship after Snowden and formulates a set of requirements for digital citizenship in a datafied environment. Having set this thematic framework, it explains the purpose of the Special Section and outlines its contributions.

Keywords: digital citizenship, surveillance, datafication, Snowden

We are digital citizens who increasingly interact with our social and political environment through digital media. Digital tools and platforms have become essential for us to participate in society. We increasingly enter the sphere of civic activity—and develop agency—through digital media.

Digital citizenship is typically defined through people's actions, rather than by their formal status of belonging to a nation-state and the rights and responsibilities that come with it. It denotes citizens creating and performing their role in society. As Isin and Ruppert note, "we are enacting ourselves in cyberspace" (Isin & Ruppert, 2015, p. 43). And just as citizens have traditionally reasserted their position in relation to the state by claiming human and civil rights, they are now "making rights claims" (Isin & Ruppert, 2015, p. 4) in the digital environment. This active construction of digital citizenship has many facets and has been widely celebrated. Scholars have discussed the democratizing effect of what has been called "liberation technology" (Diamond, 2010), such as the role of social media in political change; citizen journalism has challenged established professional media (Allan & Thorsen, 2009); fan culture has

Arne Hintz: HintzA@cardiff.ac.uk
Lina Dencik: DencikL@cardiff.ac.uk
Karin Wahl-Jorgensen: Wahl-JorgensenK@cardiff.ac.uk
Date submitted: 2017–01–02

appropriated and complemented classic cultural production (Jenkins, 2008); and surveillance scholars have analyzed "sousveillance" practices by citizens watching authorities and exposing wrongdoing (Mann, Nolan, & Wellman, 2003). Effective use of the affordances of digital, mobile and social media, it is argued, can enhance participation in society (Mossberger, Tolbert, & McNeal, 2007) and generate innovation, social change, and public good (Vivienne, McCosker, & Johns, 2016). Active digital citizenship, understood in this way, means citizen empowerment.

However, a focus on the performative and active (self-)construction of digital citizens addresses only one side of the coin. We are not just digital citizens because of our actions but also because we increasingly live and operate in a datafied environment in which everything we do leaves data traces. Many of our activities online and, increasingly, offline, generate data—geo-location data when we walk around with our mobile phone; metadata of our online communication; data on our likes and preferences; data on our movements and activities in "smart cities" and "smart homes" that are increasingly filled with sensors. This data is collected, stored, monitored, shared, and sold by social media services, other online platforms, data brokers, intelligence agencies, and public administration. Driven and sustained by an accumulation logic, this current information order has been described as "surveillance capitalism" (Zuboff, 2015).

Digital Citizenship and Datafication

For digital citizens, the monitoring and processing of their online activity may offer convenience, whether in the form of targeted advertising or personalized content geared toward their consumption habits and interests. At the same time, extensive data collection has emerged as a major challenge for digital citizenship. Under conditions of surveillance capitalism, those who hold, manage, and control the personal data of digital citizens are offered unprecedented insights into our lives, minds, and bodies. We are therefore confronted with the emergence of a new power dynamic; one that is premised on an order of "haves" and "have nots" between those who provide personal data (digital citizens) and those who own, trade, and control it (typically, large Internet companies and the state).

While much of this dynamic is facilitated by the business sector, it has significant implications for the relationship between citizens and the state. The state–citizen nexus requires careful balance to protect civic rights and liberties and to enable participation and active citizenship. However, in datafied environments, this balance is threatened as data collection empowers state agencies. As Ansorge (2016) notes, "The sovereign hungers for data. Authority demands information-generating processes to understand the social order and act on it" (p. 2). Although datafication is by no means the first instance of the state using information processing to expand its influence over citizens (Mattelart, 2003), it provides vastly enhanced possibilities to understand, predict, and control citizen activities.

In June 2013, with what can be considered the biggest intelligence leak of all time, we were made acutely aware of the nature of these new regimes of monitoring. The documents leaked by Edward Snowden, a former system administrator for the Central Intelligence Agency and information analyst at the National Security Agency (NSA), gave details of secret surveillance programs carried out by a number of Western democracies, most notably the NSA and the British Government Communications Headquarters

(GCHQ). They provided proof, for the first time, of the extent of data gathering and the different types of collecting and analyzing communications data.[1]

The Snowden leaks were not the first revelations of how states (with the help of commercial infrastructure providers) monitor people's communication. But they arrived at a critical historical juncture. Rather than merely affecting distinct items of communication (phone calls, e-mails), they have intersected with the increasingly close integration of digital technologies in our everyday lives. We now connect with our friends on apps; we share intimate information about our personal lives via chats; we vote, protest, and campaign on different platforms; and we conduct business interactions that allow us to go about our everyday life—from online banking to ordering food, transport, and lodging. Our communication devices now hold a vast range of information about our personal and professional lives, and what we like and believe is stored on the servers of social media platforms. Moreover, those devices now extend beyond computers and mobile phones to television sets, light switches, cars, and waste bins that increasingly collect, store, and process data about us. The Snowden revelations have thus intersected with the vastly increased immersion of digital technologies in every aspect of our lives and have highlighted key challenges.

Further, they coincide with broader social developments, including an ongoing fragmentation of society, a loss of cohesion based on traditional bonds, and a resulting crisis of governance of the citizenry. Classic reference points for citizenship—for example, national borders, formal organizations—have lost some of the key roles they played in traditional nation-state societies and are complemented by a wider range of often looser affiliations. Isin and Ruppert (2015) describe the digital subject as "a composite" (p. 12) of multiple forces, identifications, affiliations, and associations. Internet scholars such as Papacharissi have observed transformations of social structures from masses and collectivities to "a variety of atomized actions" (Papacharissi, 2010, p. 131). This trend intersects with the post-Fordist and neoliberal economic restructuring of the past several decades, in which centralized economic operations have given way to more complex networks of private enterprise and regulation. The differentiated and individualized social structure has provided challenges for a comprehensive overview and regulation of the citizenry by state authorities. Practices of digital surveillance offer a possibility to address this challenge. Monitoring and profiling the "atomized actions" of populations allows the state to address a fragmented reality and create a new and governable collectivity. This points us to the original (French) meaning of the word surveillance: supervision. The digital citizen is, at the same time, an active citizen and a supervised citizen.

Data collection, on a mass scale, enables a mode of governance premised on profiling, sorting, and categorizing populations in ever-proliferating ways. The state, along with corporate actors, comes to

[1] Lyon (2015) has discussed the revelations in more detail. For an overview of surveillance capabilities, see "NSA Files" by *The Guardian* (https://www.theguardian.com/us-news/the-nsa-files). For a systematic explanation of key programs, check the database developed by this project (https://www.dcssproject.net/category/technology/surveillance-programmes). For a collection of all documents leaked by Snowden, see the Snowden Surveillance Archive by Canadian Journalists for Free Expression (CJFE, https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi).

divide and compartmentalize us according to consumption habits, political preferences, or the likelihood of committing a crime. This has implications for the level of public and private services that we may receive, or the ease with which we may cross borders. In predictive policing, data on neighborhood crime rates, previous crimes of individuals, personal living conditions, and a range of other characteristics, are combined to create categories of potential future criminals (Angwin, Larson, Mattu, & Kirchner, 2016; Trottier, 2015). Credit scores and insurance rates increasingly depend on the monitoring and processing of personalized data, with the most comprehensive plan being the social media credit score that is to be rolled out in China in 2020. This will draw on citizens' social media activities, friends, messages, spending habits, and other data to determine what level of services different categories of citizens should have access to (Chin & Wong, 2016).

These new forms of categorization operate outside established categories of civic rights and offer limited, if any, possibility of redress. Moreover, they are created without our knowledge, based on criteria that do not necessarily correspond to lived experience. Even the most traditional understanding of citizenship—our nationality—has become a question of algorithmic decision making. To establish whether a piece of online communication belongs to a U.S. citizen or a foreigner (and thus is a lawful target of surveillance), the NSA analyses selectors, such as phone number, IP address, language, and the degree of interaction with people inside and outside the United States. A target is designated a foreigner, and thus a legitimate surveillance target, if at least 51% of the results from the analysis of their data suggest that they may not be a U.S. citizen (Cheney-Lippold, 2015). If someone has a U.S. passport, but communicates a lot with people from abroad, this person may be categorized as a foreigner.

Citizenship, in this case, is directly based on the data that we produce on the Internet. Cheney-Lippold refers to these designations as "jus algoritmi" thus contrasting it with classic legacies of jus sanguinis (family-based citizenship) and jus soli (location of birth). *Jus algoritmi* is "a formal, state-sanctioned enaction of citizenship that distributes political rights according to the NSA's interpretations of data" (Cheney-Lippold, 2015, p. 1729). Consequently, it "functionally abandons citizenship in terms of national identity in order to privilege citizenship in terms of provisional interpretations of data" (Cheney-Lippold, 2015, p. 1738). It sometimes aligns with a citizen's formal nationality and sometimes becomes detached from it. As the other instances of categorization, it is an identity we are assigned through data analysis, not necessarily one that we identify with or even know about.

Enabling Digital Citizenship

What, then, are the tenets of citizenship in these digitized environments? Digital citizenship is constructed partly through the enactments of users and partly through data collection and analysis. In both instances, it is dependent on particular technological, political, and social contexts. To start with, digital citizens rely on the technical infrastructure of the Internet to act and interact. This includes the "physical infrastructure" of wires and devices but also the "logical infrastructure" of standards and protocols that regulate data flows through that hardware and allow or disallow certain online activities. The code that is embedded in the infrastructure can therefore enhance or reduce the opportunities of digital citizenship (Lessig, 1999), and the institutions that develop standards and regulate data flows on the Internet play a crucial (although largely obscure) role in affecting our lives as digital citizens (Mueller,

2010). Moreover, with a growing dependence on a multitude of corporate platforms for communication, transactions, services, and information, digital citizenship is now privately and commercially mediated, and a central locus of power lies in those private organizations (Hintz, 2015). Digital citizens are increasingly bound not just by legality and by constitutional rights, but by the "benevolence" (Leistert, 2015, p. 36) of commercial entities.

In this complex environment of different types and levels of infrastructure, digital citizenship would require adequate protection of Internet users' basic rights, such as freedom of expression and privacy. While protocols and standards, as well as the terms of service of (and the algorithms used by) online platforms, constitute important parts of this policy environment, national laws and regulations continue to provide necessary cornerstones, in combination with regional policies (e.g., at EU level) and transnational rule making (e.g., in the institutions of global Internet governance; Hintz & Dencik, 2016). A supportive legal and regulatory framework for secure online interactions is thus a further important condition for digital citizenship.

Moreover, if digital citizenship is based on active users, crowdsourcing, and participation, its meaningful enactment requires an informed and knowledgeable understanding of the technologies in place and how they might be used. Here, the watchdog function we traditionally attribute to journalism is critical. In the context of the Snowden revelations, this means that news media would need to convey detailed information on how state agencies intervene into digital communication and what this means for the daily activities of digital citizens. As a result, users would be aware of both the opportunities and risks of engaging with digital environments, and know how to both protect and claim their rights in cyberspace.

An ideal configuration of digital citizenship would therefore be based on the possibility of comprehensive self-determination in a datafied environment, provided by secure infrastructure, an enabling regulatory environment, adequate public knowledge, and an informed use of the relevant platforms and applications.

Researching Digital Citizenship and Surveillance

To investigate these components and conditions of digital citizenship, an interdisciplinary research team conducted the collaborative project, Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks, between 2014 and 2016. The project analyzed the implications of the Snowden leaks across four different thematic areas that we identified as technology, policy, news media, and civil society. In doing this, we sought to explore the state of digital citizenship in the immediate aftermath of the Snowden leaks in light of the technical infrastructures and standards; the legal and regulatory framework of surveillance; media coverage of the leaks; and public knowledge and attitudes about surveillance. The research involved a combination of qualitative and quantitative methods, including policy document analysis, focus groups, expert interviews, and media content analysis.

The project was hosted at the School of Journalism, Media and Cultural Studies at Cardiff University, and it was funded by the UK Economic and Social Research Council. The main investigators were Arne Hintz, Lina Dencik, Karin Wahl-Jorgensen (all Cardiff University), Ian Brown (Oxford University)

and Michael Rogers (Briar Project). The work included the international conference Surveillance and Citizenship at Cardiff University on June 18–19, 2015, and a number of presentations at academic, industry and civil society events (see the project website: http://www.dcssproject.net).

The research has provided a multifaceted analysis of the state of digital citizenship in the aftermath of the Snowden leaks. It has, in particular, expanded on established notions of digital citizenship, focused on its active and empowering nature, by investigating the challenges that arise from mass collection and processing of data. As the research results have shown, the Snowden leaks have crystallized a shift in the meaning of citizenship. Enactments of citizenship are now predominantly carried out within a monitored environment that seeks to sort and categorize individuals and allows for increased control over their activities. Although the Snowden leaks and subsequent events have created spaces for transparency and potentials for challenge and critique with regards to mass data collection, the research also illustrates the extent to which possibilities for change have been stifled by limited public debate and knowledge, feelings of disempowerment, and systematic reinforcement of state and corporate interests over and above those of citizens. This puts a substantial question mark over the extent to which our current digital environment enables citizenship in a meaningful way.

Contributions to This Special Section

This Special Section is organized around three distinct parts. The first four articles present and discuss the research results developed as part of the project, Digital Citizenship and Surveillance Society, according to the four project themes mentioned earlier. To start off this group of articles, Karin Wahl-Jorgensen, Lucy Bennett, and Gregory Taylor explore the distinctive ways in which UK-based newspapers and blogs constructed debates over surveillance in the aftermath of the Snowden revelations. They demonstrate that newspapers have normalized surveillance by highlighting concerns over national security and focusing on surveillance of elites. This, in turn, means that mass surveillance of citizens is much less prominent in coverage. By contrast, blogs and specialist online publications have opened up a space for critical discussions relevant to digital citizenship, by enabling debates on civil rights and privacy.

Following this, Lina Dencik and Jonathan Cable explore the nature of understandings and attitudes toward surveillance in light of the Snowden leaks among the general public as well as political activists. They identify a significant level of unease with ubiquitous data collection but also a sense of resignation to its inevitability, coupled with widespread confusion as to the purpose, degrees, and practices of surveillance. They argue that this speaks to what they call "surveillance realism"—a condition in which imagining alternative ways of organizing society has become increasingly difficult.

Arne Hintz and Ian Brown turn to the policy environment of surveillance by zooming in on a particular policy reform process in the United Kingdom. As a consequence of the Snowden revelations, the UK government developed a comprehensive legislative framework to regulate the activities of intelligence and security agencies—the Investigatory Powers Bill. Hintz and Brown, in their article, trace the forces and dynamics that have shaped this particular policy response, investigate key controversies over the types and extent of surveillance, and analyze the capacity of different stakeholders to intervene into the debate

and shape its outcomes. They conclude that the new law does not reflect the full range of concerns and leaves digital citizenship in a more precarious state.

Finally, Michael Rogers and Grace Eden address the question of infrastructure by focusing on Internet standards and investigating the struggle between those who seek to encode surveillance capabilities in the infrastructure and those who wish to protect user privacy. They document how the NSA has manipulated technical standards to render communication infrastructures susceptible to surveillance, and how standards bodies have responded. Based on this analysis, they discuss the adequacy and legitimacy of current mechanisms for negotiating standards.

These four articles summarizing research results from the specific project are complemented and contextualized by four articles from renowned scholars across the fields of surveillance and digital media. David Lyon situates the specific implications of the Snowden revelations in the concepts of "surveillance culture," "surveillance imaginaries," and "surveillance practices." In particular, he explores the online practice of "sharing" and its implications of visibility and exposure to examine how today's subjects themselves make sense of, respond to, and in some cases initiate surveillance activities. Turning the perspective from the state to the citizen, he thereby offers a missing link in the discussion of digital citizenship. Engin Isin and Evelyn Ruppert continue this engagement with the digital citizen, but focus on Snowden himself. Asking what kind of citizenship he has performed, they discuss the theory of performative citizenship beyond the nation-state and conclude that he performed a kind of citizenship that is yet to come. In part, it is international, and in part, it focuses on making digital rights claims that do not yet exist in law. The authors argue that Snowden's act called for digital rights and responsibilities that traverse national legal orders.

Adrienne Russell and Silvio Waisbord return to the theme of media coverage and public debate by investigating the dynamics of the networked fourth estate. They employ the notion of news flashpoints to explore how debates moved across various types of news media and platforms and across professional-amateur-special interest borders. They demonstrate how stories related to the leaks were sustained and broadened in this hybrid environment and consider the implications for the public. Moving beyond the theme of the Snowden revelations, Mark Andrejevic explores the implications of recent developments in predictive policing for the relationship between citizenship and surveillance. Through this case study, he identifies emerging practices of environmental surveillance that rely on actuarial modes of prediction. The growing emphasis on strategies for preemption rather than on policies for prevention, he argues, displaces political deliberation with technological expertise and work in the direction of automated decision making about resources allocation and armed response. The article therefore points to current and future trajectories in the study of digital citizenship.

The collection of eight academic articles in this Special Section is complemented by insights from two key figures in the post-Snowden debate. Ben Wizner from the American Civil Liberties Union—more prominently known as Snowden's lawyer—asks whether the Snowden revelations have changed the ways in which surveillance is implemented, regulated, and accepted. Focusing on the United States and adopting a positive perspective, he argues that courts, Congress, media, and technology companies have substantially altered their behavior after the beginning of the disclosures. Institutions that may serve as

counterweight to the security state were therefore strengthened and have challenged surveillance practices. Gus Hosein, executive director of Privacy International, concludes the section by questioning one of the central truisms of the post-Snowden debate: an alleged trade-off between human rights and security that digital citizens need to negotiate, and a balance between both that supposedly needs to be struck by policy makers. Hosein problematizes the—often uncritical—discussion over an alleged balance by addressing the recent conflict between Apple and the FBI over the encryption of mobile phones.

Together, the 10 articles of this Special Section seek to advance our understanding of digital citizenship in times of datafication and ubiquitous online surveillance. They open up avenues for a critical investigation into the conditions, contexts, and practices of digital citizenship at this historical juncture.

References

Allan, S., & Thorsen, E. (2009). *Citizen journalism: Global perspectives.* New York, NY: Peter Lang.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias. *Pro Publica.* Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Ansorge, J. (2016). *Identify and sort: How digital power changed world politics.* London, UK: Hurt & Company.

Cheney-Lippold, J. (2015). Jus algoritmi: How the National Security Agency remade citizenship. *International Journal of Communication, 10*(2016), 1721–1742. Retrieved from http://ijoc.org/index.php/ijoc/article/view/4480/1618

Chin, J., & Wong, G. (2016, November 28). China's new tool for social control: A credit rating for everything. *The Wall Street Journal.* Retrieved from http://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590

Diamond, L. (2010). Liberation technology. *Journal of Democracy, 21*(3), 69–83.

Hintz, A. (2015). Social media censorship, privatised regulation, and new restrictions to protest and dissent. In L. Dencik & O. Leistert (Eds.), *Critical perspectives on social media and protest: Between control and emancipation* (pp. 109–126). Lanham, MD: Rowman & Littlefield.

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review, 5*(3). Retrieved from https://policyreview.info/articles/analysis/politics-surveillance-policy-uk-regulatory-dynamics-after-snowden

Isin, E., & Ruppert, E. (2015). *Becoming digital citizens*. Lanham, MD: Rowman & Littlefield.

Jenkins, H. (2008). *Convergence culture: Where old and new media collide.* New York: New York University Press.

Leistert, O. (2015). The revolution will not be liked: On the systematic constraints of corporate social media platforms for protest. In L. Dencik & O. Leistert (Eds.), *Critical perspectives on social media and protest: Between control and emancipation* (pp. 35–52). Lanham, MD: Rowman & Littlefield.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

Lyon, D. (2015). *Surveillance after Snowden.* Cambridge, UK: Polity Press.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

Mattelart, A. (2003). *The information society.* London, UK: SAGE Publications.

Mossberger, K., Tolbert, C., & McNeal, R. S. (2007). *Digital citizenship: The Internet, society, and participation*. Cambridge, MA: MIT Press.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Cambridge, UK: Polity Press.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4/5), 530–547.

Vivienne, S., McCosker, A., & Johns, A. (2016). Digital citizenship as fluid interface: Between control, contest and culture. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating digital citizenship: Control, contest and culture* (pp. 1–18). London, UK: Rowman & Littlefield.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.